Agnieszka Grzelak
Akademia Leona Koźmińskiego
agrzelak@alk.edu.pl
ORCID: 0000-0002-5867-8135

https://doi.org/10.26881/gsp.2021.4.03

Przyszłość współpracy UE z państwami trzecimi w sprawie przekazywania danych pasażerów lotniczych. O skutkach opinii Trybunału Sprawiedliwości nr 1/15 dla wymiany danych PNR

1. Wprowadzenie

Problematyka przetwarzania danych PNR (*Passenger Name Record*) jest przedmiotem badań naukowych i praktyki od lat. Instrumenty PNR są bowiem doskonałym przykładem dychotomii między prywatnością a bezpieczeństwem publicznym[1]. Jest to również atrakcyjny instrument zwalczania terroryzmu i poważnej przestępczości, stąd też nie dziwi, że zawarciem umów pozwalających na przetwarzanie danych jest zainteresowanych szereg państw, a prace nad wypracowaniem standardów prowadzą organizacje międzynarodowe[2].

Dane PNR to zbiór danych o podróży każdego pasażera linii lotniczych, który zawiera informacje niezbędne, aby umożliwić przetwarzanie i weryfikowanie rezerwacji przez przewoźników lotniczych obsługujących lot w odniesieniu do każdego przelotu zarezerwowanego przez jakąkolwiek osobę lub w jej imieniu. Dane te są przekazywane przez pasażerów przewoźnikom lotniczym podczas dokonywania rezerwacji na lot[3]. Dane PNR należy przy tym odróżnić od tzw. danych API (*Advance Passenger*

[1] H. Hijmans, *PNR Agreement EU-Canada Scrutinised: CJEU Gives Very Precise Guidance to Negotiators*, „European Data Protection Law Review" 2017, nr 3, s. 406.

[2] Poza UE należy do nich chociażby International Civil Aviation Organisation ICAO, która już w 2010 r. przyjęła wytyczne: Guidelines on Passenger Name Record (PNR) Data, doc. 9944 https://www.icao.int/Security/FAL/ANNEX9/Documents/9944_cons_en.pdf [dostęp: 25.11.2021]. Od marca 2019 r. trwają prace nad nowym dokumentem ICAO. Również Rada Bezpieczeństwa ONZ w 2017 r. uchwalił rezolucję, która zobowiązuje państwa do rozwoju systemu przetwarzania danych PNR: United Nations Security Council Resolution 2396 (2017).

[3] Zob. m.in. definicję danych PNR zawartą w dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania (Dz. Urz. UE L 119, s. 132).

Information), czyli danych biograficznych pobranych z części paszportu możliwej do automatycznego odczytu, która obejmuje imię i nazwisko, miejsce zamieszkania, miejsce urodzenia i obywatelstwo osoby. Wykorzystanie danych PNR znacząco różni się od sposobu wykorzystywania danych API – dane PNR są raczej narzędziem służącym walce z przestępczością, a nie weryfikacji tożsamości w związku z przekroczeniem granicy. Dane PNR służą do oceny ryzyka związanego z przelotem pasażera, czy też do identyfikacji osób, które mogą być podmiotem zainteresowania organów ścigania, a także osób powiązanych z osobą podejrzewaną o popełnienie przestępstwa[4].

W ostatnim dziesięcioleciu na forum UE podjęto działania zmierzające po pierwsze, do uregulowania zasad przekazywania danych PNR z UE do państw trzecich, jak również do stworzenia wewnątrzunijnej regulacji dotyczącej PNR. Jednocześnie bardzo w tych latach wzmocnił się poziom ochrony prawa do prywatności i prawa do ochrony danych osobowych, co bez wątpienia miało wpływ nie tylko na działania Komisji Europejskiej, ale przede wszystkim znalazło swój wyraz w orzeczeniach Trybunału Sprawiedliwości (TS, Trybunał)[5]. Wejście w życie Traktatu z Lizbony nie tylko wiązało się z przyznaniem mocy prawnej równej traktatom: Karcie Praw Podstawowych UE (KPP), wprowadzeniu do Traktatu o funkcjonowaniu Unii Europejskiej nowego art. 16 TFUE[6], ale także oznaczało zmianę procedury zawierania umów międzynarodowych tego typu (konieczność uzyskania zgody Parlamentu Europejskiego)[7]. Przypomnienie tych

[4] Ciekawego podsumowania definicji i znaczenia danych PNR dokonuje T. Maruhashi, *Japan-EU Passenger Name Record Negotiations and Their Implications* [w:] *Human-Centric Computing in a Data-Driven Society. 14th IFIP TC 9 International Conference on Human Choice and Computers*, red. D. Kreps, T. Komukai, T.V. Gopal, K. Ishii, HCC14 2020, Tokyo, Japan, September 9–11, 2020, Proceedings, Springer 2020, s. 100 i n.

[5] Wystarczy tu wspomnieć o tych orzeczeniach, które będą punktem wyjścia dla TS w sprawie opinii 1/15: wyrok Trybunału (wielka izba) z dnia 8 kwietnia 2014 r. w sprawach połączonych C-293/12 i C-594/12 *Digital Rights Ireland Ltd przeciwko Minister for Communications, Marine and Natural Resources i in.* oraz *Kärntner Landesregierung i in.*, ECLI:EU:C:2014:238; dalej: wyrok w sprawie DRI; wyrok Trybunału (wielka izba) z dnia 6 października 2015 r. w sprawie C-362/14 *Maximillian Schrems przeciwko Data Protection Commissioner*; dalej: wyrok w sprawie Schrems I, ECLI:EU:C:2015:650 czy wyrok TS z dnia 21 grudnia 2016 r. w sprawach połączonych C-203/15 i C-698/15, *Tele2 Sverige AB przeciwko Post- och telestyrelsen* oraz *Secretary of State for the Home Department przeciwko Tomowi Watsonowi, Peterowi Brice'owi, Geoffrey'owi Lewisowi*, EU:C:2016:970 Nie można jednak zapominać o najnowszych orzeczeniach z dnia 6 października 2020 r. w sprawach C-623/17, *Privacy International przeciwko Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service*, EU:C:2020:790, dalej: wyrok C-623/17, *Privacy International*; wyrok TS z dnia 6 października 2020 r., sprawy połączone C-511/18, C-512/18 i C-520/18, *La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net przeciwko Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées oraz Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX przeciwko Conseil des ministres*, EU:C:2020:791; dalej: wyrok w sprawach połączonych C-511/18, C-512/18 i C-520/18, *La Quadrature du Net*.

[6] Na ten temat szerzej A. Grzelak, *Prawo do ochrony danych osobowych a konieczność walki z przestępczością. Uwagi na tle art. 16 traktatu o funkcjonowaniu Unii Europejskiej* [w:] *Prawo Unii Europejskiej a prawo konstytucyjne państw członkowskich*, red. S. Dudzik, N. Półtorak, Warszawa 2013, s. 407–434.

[7] Por. obecny art. 218 ust. 6 TFUE.

działań będzie przedmiotem pierwszego fragmentu niniejszego artykułu. Przyjmowanie kolejnych aktów prawnych wiązało się jednak z szeregiem wątpliwości i zastrzeżeń dotyczących poziomu ochrony praw podstawowych, w szczególności prawa do prywatności i prawa do ochrony danych osobowych. Zasadnicze uwagi zgłaszane były przez Europejskiego Inspektora Ochrony Danych (EDPS) czy też przez organizacje pozarządowe. Szereg z tych problemów stało się przedmiotem analizy Trybunału Sprawiedliwości w jednym z najważniejszych orzeczeń z tej dziedziny w ostatnich latach, a mianowicie w opinii 1/15 dotyczącej projektowanej umowy w sprawie przekazywania danych PNR, która miała być zawarta z Kanadą[8]. Te problemy będą przedmiotem analizy w następnej części opracowania, a opinia 1/15 powinna stać się kluczowym punktem odniesienia dla wszelkich dalszych analiz. Podstawowym jednak zagadnieniem, które jest przedmiotem niniejszego tekstu będzie próba odpowiedzi na pytanie o znaczenie opinii 1/15 dla dalszych prac nad systemem PNR i przyszłość współpracy z państwami trzecimi w tym obszarze, ale także jej znaczenie dla całego systemu ochrony danych osobowych w Unii Europejskiej.

2. Ewolucja prac nad systemem PNR w kontekście zewnętrznym i wewnętrznym w Unii Europejskiej – krótkie przypomnienie

Zanim przedstawione zostaną podstawowe problemy związane z uregulowaniem zasad przekazywania danych PNR do państw trzecich, określone w orzecznictwie Trybunału, warto krótko uporządkować ewolucję prac nad systemem PNR zarówno w kontekście zewnętrznym (negocjacji z państwami trzecimi), jak i wewnętrznym (stworzeniem systemu EU-PNR).

Komisja Europejska rozpoczęła prace nad uregulowaniem zasad gromadzenia danych PNR przez przewoźników i przekazywania ich właściwym organom odpowiedzialnym za zwalczanie przestępczości, wnosząc w roku 2003[9] o ustanowienie bezpiecznych pod względem prawnym ram dla przekazywania PNR do Departamentu Bezpieczeństwa Wewnętrznego USA (*Department of Homeland Security* – DHS) oraz do przyjęcia wewnętrznej polityki w zakresie PNR. Konieczność podjęcia działań w tym zakresie była związana z polityką wewnętrzną USA, gdzie krótko po wydarzeniach z 11 września 2001 r. wprowadzono regulacje zobowiązujące przewoźników lotniczych (w tym unijnych) do przekazywania danych władzom amerykańskim[10]. Pracom nad umową z USA towarzyszyły zastrzeżenia Parlamentu Europejskiego (PE) i Grupy Roboczej Art. 29, która wnosiła o zapewnienie adekwatnego poziomu ochrony w USA[11].

[8] Opinia Tybunału (wielka izba) 1/15 z dnia 26 lipca 2017 r., ECLI:EU:C:2017:592; dalej: opinia 1/15.

[9] Komunikat do Rady i Parlamentu w sprawie przekazywania danych dotyczących przelotu pasażera (PNR): globalne podejście UE, COM(2003) 826.

[10] P.M. Schwartz, *The EU-US Privacy Collission: A Turn to Institutions and Procedures*, Harvard Law Review 2013, s. 1973–1979.

[11] Negocjacje rozpoczęte z USA zakończyły się zawarciem umowy przez Radę pomimo tego, że Parlament Europejski chciał opinii TS dotyczącej podstawy prawnej porozumienia. Ostatecznie jednak

Odpowiednie skargi trafiły do Trybunału Sprawiedliwości i w 2006 r. TS unieważnił decyzję Rady dotyczącą zawarcia umowy oraz decyzję Komisji o adekwatnym poziomie ochrony[12], przy czym powodem nie były kwestie merytoryczne (TS nie dokonywał analizy), lecz wybór niewłaściwej podstawy prawnej. Dalsze negocjacje doprowadziły do podpisania przez UE umowy ze Stanami Zjednoczonymi Ameryki o przekazywaniu danych PNR w interesie walki z terroryzmem i poważną przestępczością transgraniczną, która to umowa zapewnia przekazywanie danych PNR, przy jednoczesnej ochronie danych osobowych[13]. W tym okresie podpisane zostały również umowy z Kanadą i Australią (które ostatecznie były stosowane tymczasowo)[14].

Kolejny komunikat dotyczący globalnego podejścia do przekazywania danych dotyczących przelotu pasażera (PNR) państwom trzecim Komisja przedstawiła w 2010 r.[15], proponując dalsze działania w odpowiedzi na ataki terrorystyczne w Stanach Zjednoczonych, w Madrycie i Londynie, a także w związku z potrzebą wzmocnienia poszanowania praw podstawowych. Komisja zaprezentowała w nim globalne podejście do transferów danych PNR do państw trzecich, ustanawiając zestaw kryteriów, które muszą być spełnione odnośnie do zasad i gwarancji bezpieczeństwa danych. W efekcie, w wymiarze zewnętrznym obecnie stan umów i etapy negocjacyjne prezentują się następująco[16]:

---

wycofał swój wniosek o zbadanie treści umowy, a zamiast tego wniósł o stwierdzenie nieważności decyzji Rady o zawarciu umowy. Na ten temat szerzej: E. Guild, E. Brouwer, *The ECJ Decision on the PNR Agreement between the EU and the US*, CEPS Policy Brief July 2006, nr 109 oraz M. Mendez, *Passenger Name Record Agreement*, European „Constitutional Law Review" 2007, vol. 3, nr 1, s. 127, a także V. Papakonstantinou, P. de Hert, *The PNR Agreement and Transatlantic Anti-Terrorism Cooperation: No Firm Human Rights Framework on Either Side of the Atlantic*, „Common Market Law Review" 2009, s. 885.

[12] Wyrok Trybunału (wielka izba) z dnia 30 maja 2006 r. w połączonych sprawach Parlament Europejski przeciwko Radzie Unii Europejskiej (C-317/04) i Komisji Wspólnot Europejskich (C-318/04), Zb. Orz. 2006, I-04721, ECLI:EU:C:2006:346. Trybunał Sprawiedliwości uniknął odpowiedzi na pytania co do zgodności umowy z zasadami ochrony danych osobowych, stwierdzając jedynie, że nieprawidłowo wskazano podstawę prawną decyzji Rady, co w efekcie naruszało uprawnienia Parlamentu. Co zaskakujące, w opinii rzecznika generalnego porozumienie zostało uznane za zgodne ze standardem wynikającym z art. 8 EKPC. Zob. opinię z 22.11.2005 r., ECLI:EU:C:2005:710.

[13] Decyzja Rady 2007/551/WPZiB/WSiSW z dnia 23 lipca 2007 r. w sprawie podpisania, w imieniu Unii Europejskiej, Umowy między Unią Europejską a Stanami Zjednoczonymi Ameryki o przetwarzaniu i przekazywaniu przez przewoźników lotniczych danych dotyczących przelotu pasażera (PNR) do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych (DHS) (Umowa PNR z 2007 r.) oraz Umowa między Unią Europejską a Stanami Zjednoczonymi Ameryki o przetwarzaniu i przekazywaniu przez przewoźników lotniczych danych dotyczących przelotu pasażera (PNR) do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych (DHS) (Umowa PNR z 2007 r.), Dz. Urz. L 204, s. 16 i s. 18.

[14] Dz. Urz. UE L 91 z 2006 r., s. 53, s. 49; Dz. Urz. UE L 82 z 2006 r., s. 15 oraz Dz. Urz. UE L 213 z 2008 r., s. 49.

[15] Zob. komunikat Komisji z 21.09.2010 r. w sprawie globalnego podejścia do przekazywania danych dotyczących przelotu pasażera (PNR) państwom trzecim, COM(2010) 492 final.

[16] Stan na dzień: 18.06.2021 r.

Tab. 1. Umowy zawarte między UE a państwami trzecimi – obowiązujące

Państwo	Data podpisania umowy	Data wejścia w życie	Dodatkowe raporty lub informacje
Australia[17]	29 września 2011 r.	1 czerwca 2012 r.	sprawozdanie z 2014 r.[18] sprawozdanie z 2021 r.[19]
USA	14 grudnia 2011 r.[20]	1 lipca 2012 r.	sprawozdanie z 2017 r.[21] sprawozdanie z 2021 r.[22]

Źródło: Opracowanie własne.

Tab. 2. Trwające negocjacje

Państwo	Data rozpoczęcia negocjacji	Aktualna sytuacja
Kanada	25 czerwca 2014 r. – podpisanie umowy	w świetle opinii TSUE 1/15 umowa w tej formie nie może być zawarta
	czerwiec 2018 r.	rozpoczęcie negocjacji nad nową umową
Meksyk	2015 r.[23]	negocjacje zawieszone
Japonia	18 lutego 2020 r.	decyzja Rady o rozpoczęciu negocjacji[24]

Źródło: Opracowanie własne.

[17] Umowa między Unią Europejską a Australią o przetwarzaniu i przekazywaniu przez przewoźników lotniczych australijskiej służbie celnej i granicznej danych dotyczących przelotu pasażera (danych PNR) (Dz. Urz. UE L 186 z 2012 r., s. 4.).

[18] Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady w sprawie wspólnego przeglądu realizacji Umowy między Unią Europejską a Australią o przetwarzaniu i przekazywaniu przez przewoźników lotniczych australijskiej służbie celnej i granicznej danych dotyczących przelotu pasażera (danych PNR), COM(2014) 458 final.

[19] Report from the Commission to the European Parliament and the Council: On the joint review of the implementation of the Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, COM(2021) 19 final.

[20] Umowa między Stanami Zjednoczonymi Ameryki a Unią Europejską o wykorzystywaniu danych dotyczących przelotu pasażera oraz przekazywaniu takich danych do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych (Dz. Urz. UE L 215 z 2012 r., s. 5).

[21] Report from the Commission to the European Parliament and the Council: On the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security COM(2017) 29 final.

[22] Report from the Commission to the European Parliament and the Council on the joint evaluation of the Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, COM(2021) 18 final.

[23] https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_15_5374 [dostęp: 25.11.2021].

[24] https://www.consilium.europa.eu/pl/press/press-releases/2020/02/18/eu-japan-pnr-agreement-council-authorises-opening-of-negotiations/ [dostęp: 25.11.2021].

Równolegle rozpoczęto prace nad stworzeniem europejskiego systemu przekazywania danych PNR (tzw. EU-PNR), najpierw przedstawiając projekt decyzji ramowej Rady[25], a następnie – w związku z wejściem w życie Traktatu z Lizbony – projekt dyrektywy, nad którą prace zakończyły się w 2016 r. przyjęciem dyrektywy 2016/681 (dyrektywa EU-PNR)[26]. Dyrektywę przyjęto, chociaż opinia Europejskiego Inspektora Ochrony Danych (EDPS) była w tym zakresie negatywna – w jego ocenie zachodziła sprzeczność proponowanych przepisów ze standardem wynikającym z Karty Praw Praw Podstawowych (KPP, Karta)[27]. Dyrektywa definiuje zadania państw członkowskich w zakresie przetwarzania danych PNR, wymagając od nich m.in. ustanowienia jednostek odpowiedzialnych za zbieranie, przechowywanie i przetwarzanie danych (tzw. jednostki PIU – *passenger information units*) oraz do przyjęcia listy organów właściwych do wnioskowania o dostęp i otrzymywania danych PNR. Zasady określone w dyrektywie stosuje się w odniesieniu do lotów z państw trzecich do UE, jednak państwa członkowskie UE mogą podjąć decyzję o zastosowaniu ich również w odniesieniu do lotów wewnątrzunijnych[28]. W dniu 24 lipca 2020 r. Komisja przestawiła Parlamentowi Europejskiemu i Radzie sprawozdanie dotyczące przeglądu dyrektywy 2016/681 w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania[29]. Ogólna ocena dotycząca pierwszych miesięcy stosowania przepisów jest pozytywna, działania państw w kierunku jej implementacji ogólnie zadowalajace, a dyrektywa nie wymaga na tym etapie żadnych zmian. Tymczasem ocena poszczególnych rozwiązań i sposobu ich wdrożenia do prawa krajowego przez badaczy do takich entuzjastycznych wniosków już nie prowadzi, o czym jeszcze będzie mowa w dalszej części tekstu.

Wydanie przez Trybunał Sprawiedliwości wspomnianej we wprowadzeniu do niniejszego tekstu opinii 1/15, która będzie jeszcze przedmiotem analizy w dalszej części, zdecydowanie przyhamowało proces negocjowania i zawierania umów z państwami trzecimi i wymusiło na Komisji konieczność przedstawienia nowego podejścia i dostosowania się do wymogów wynikających z orzecznictwa. Komisja w dniu

[25] W 2007 r. Komisja przedstawiła wniosek dotyczący projektu decyzji ramowej regulującej omawiane zagadnienia, COM(2007) 654 final.

[26] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania (Dz. Urz. UE L 119, s. 132; dalej: dyrektywa EU-PNR albo dyrektywa 2016/681).

[27] Opinia EDPS 5/2015 z dnia 24 września 2015 r., https://edps.europa.eu/sites/default/files/publication/15-09-24_pnr_en.pdf [dostęp: 25.11.2021].

[28] Zob. zaktualizowaną listę państw członkowskich, które podjęły decyzję o stosowaniu dyrektywy w sprawie wykorzystywania danych PNR do lotów wewnątrzunijnych zgodnie z art. 2 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/681 w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania (Dz. Urz. UE C 358 z 2020 r., s. 7). Na tej liście znajduje się Polska.

[29] COM(2020) 305 final.

24 lipca 2020 r. opublikowała zatem tzw. mapę drogową[30], w której podsumowała rozwój sytuacji dotyczącej stosowania danych PNR na świecie od 2010 r., a także dokonała próby określenia polityki dotyczącej przekazywania danych PNR państwom spoza UE. Podstawowym problemem, jaki zarysował się w ostatnim dziesięcioleciu były bowiem różnice w standardzie ochrony danych osobowych i prywatności pomiędzy Unią Europejską (zwłaszcza w związku z reformą dokonaną w 2016 r.) a państwami trzecimi[31].

3. Prace nad umową z Kanadą i wniosek Parlamentu Europejskiego do TSUE

Pierwsza umowa z Kanadą została zawarta już w 2005 r. pomimo tego, że już na tym etapie pojawiały się wątpliwości dotyczące standardu ochrony prawa do prywatności i danych osobowych[32]. W dniu 18 lipca 2005 r. Rada przyjęła decyzję 2006/230/WE w sprawie zawarcia umowy pomiędzy Wspólnotą Europejską a rządem Kanady o przetwarzaniu danych API/PNR[33], którą zatwierdziła tę umowę. Zgodnie z preambułą, została ona zawarta z uwzględnieniem wymogu rządu Kanady, który to wymóg dotyczył przekazywania przez przewoźników lotniczych właściwym władzom Kanady informacji o pasażerach oraz zapisu danych dotyczących nazwiska pasażera (danych „API/PNR") w zakresie, w jakim są one zbierane i zawarte w automatycznych systemach rezerwacji oraz odprawy, należących do przewoźników. Celem tej umowy było zapewnienie, by dane API/PNR były przekazywane przy pełnym poszanowaniu podstawowych praw i wolności, w szczególności prawa do prywatności.

W dniu 6 września 2005 r. Komisja przyjęła decyzję 2006/253/WE w sprawie odpowiedniej ochrony danych osobowych zawartych w Imiennym Rejestrze Pasażerów linii lotniczych, przekazanym do Agencji Służb Granicznych Kanady (CBSA)[34]. Zgodnie z tą decyzją, CBSA miała zapewnić odpowiedni poziom ochrony danych PNR przekazywanych z Unii Europejskiej w związku z lotami do Kanady, zgodnie wymogami określonymi w załączniku do decyzji. Decyzja ta miała obowiązywać przez trzy lata i sześć miesięcy od daty podania jej do wiadomości – przy czym do przedłużenia obowiązywania

30 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12531-External-dimension-of-the-EU-policy-on-Passenger-Name-Records-_pl [dostęp: 14.06.2021].

31 Zob. w szczególności wyrok Trybunału Sprawiedliwości w sprawie *Schrems II*: wyrok z 16.07.2020 w sprawie C-311/18 *Data Protection Commissioner przeciwko Facebook Ireland Limited i Maximillianowi Schremsowi*, ECLI:EU:C:2020:559.

32 Na jej temat zob. bardzo szeroko P. Hobbing, *Tracing Terrorists: The EU-Canada Agreement in PNR Matters* CEPS Special Report, September 2008 Revised version 17.11.2008, http://aei.pitt.edu/11745/1/1704.pdf [dostęp: 18.06.2021]. Zob. również opinię Europejskiego Inspektora Ochrony Danych w sprawie wniosku dotyczącego decyzji Rady w sprawie zawarcia porozumienia pomiędzy Wspólnotą Europejską a Rządem Kanady w sprawie przetwarzania zaawansowanych informacji na temat pasażerów (API) oraz danych dotyczących nazwy rekordu pasażera (PNR) (COM(2005) 200 wersja ostateczna), Dz. Urz. UE C 218 z 2005 r., s. 6.

33 Dz. Urz. UE L 82 z 2006 r., s. 14.

34 Dz. Urz. UE L 91 z 2006 r., s. 49.

tej decyzji nie doszło. Okres obowiązywania umowy z 2006 r. był zgodnie z art. 5 ust. 1 i ust. 2 związany był z okresem obowiązywania decyzji 2006/253, a zatem termin obowiązywania tej umowy upłynął we wrześniu 2009 r. i pojawiła się potrzeba rozpoczęcia rozmów na temat nowej umowy.

W dniu 5 maja 2010 r. Parlament Europejski przyjął rezolucję dotyczącą rozpoczęcia negocjacji w sprawie umów dotyczących rejestru nazwisk pasażerów (PNR) ze Stanami Zjednoczonymi, Australią i Kanadą[35], zaś pół roku później Rada przyjęła decyzję upoważniającą Komisję do rozpoczęcia w imieniu Unii negocjacji z Kanadą w sprawie umowy o przekazywaniu i przetwarzaniu danych dotyczących przelotu pasażera w celu zapobiegania terroryzmowi i innych poważnych przestępstw międzynarodowych oraz ich zwalczania, a także wytyczne negocjacyjne w tej sprawie. Umowa została parafowana w dniu 6 maja 2013 r. W dniu 5 grudnia 2013 r. Rada przyjęła decyzję w sprawie podpisania umowy między Kanadą a Unią Europejską o przekazywaniu i przetwarzaniu danych dotyczących przelotu pasażera. Przewidywana umowa została podpisana w dniu 25 czerwca 2014 r., a kilka dni później Rada zwróciła się do PE o wyrażenie zgody na projekt decyzji Rady w sprawie zawarcia przewidywanej umowy.

W dniu 25 listopada 2014 r. Parlament Europejski przyjął rezolucję w sprawie zasięgnięcia opinii Trybunału Sprawiedliwości na temat zgodności z traktatami umowy między Kanadą a Unią Europejską w sprawie przekazywania i przetwarzania danych dotyczących przelotu pasażera[36]. Wniosek PE o wydanie opinii dotyczył zarówno zgodności przewidywanej umowy z prawem pierwotnym Unii, jak i właściwej podstawy prawnej decyzji Rady dotyczącej zawarcia przewidywanej umowy i miał następujące brzmienie:

„Czy projekt przewidywanej umowy jest zgodny z postanowieniami traktatów (art. 16 TFUE) i Kartą praw podstawowych Unii Europejskiej (art. 7, 8 i art. 52 ust. 1) w zakresie prawa osób fizycznych do ochrony danych osobowych?

Czy art. 82 ust. 1 lit. d) oraz art. 87 ust. 2 lit. a) TFUE stanowią właściwą podstawę prawną aktu Rady dotyczącego zawarcia przewidywanej umowy, czy też akt ten należy oprzeć na podstawie prawnej z art. 16 TFUE?".

W ten sposób, na podstawie art. 218 ust. 11 TFUE, umowa z Kanadą trafiła do Trybunału Sprawiedliwości, który miał wypowiedzieć się na temat jej zgodności z przepisami TFUE i KPP UE. Zanim zapadł wyrok, opinię w tej sprawie przedstawił rzecznik generalny Paolo Mengozzi, który zaproponował, by Trybunał uznał część przepisów umowy za niezgodne z art. 7, 8 i 52 ust. 1 KPP ze względu na wykroczenie poza to, co ściśle konieczne, brak precyzji, naruszenie zasady celowości i zbyt długi okres retencji danych[37].

---

[35] Dz. Urz. UE C 81 z 2011 r., s. 70.

[36] Dz. Urz. UE C 289 z 2016 r., s. 2.

[37] Opinia rzecznika generalnego P. Mengozziego przedstawiona 8.09.2016 r. w sprawie 1/15, EU:C:2016:656.

4. Opinia 1/15 Trybunału Sprawiedliwości

Trybunał Sprawiedliwości swoją opinię przedstawił 26 lipca 2017 r. W pierwszej kolejności Trybunał Sprawiedliwości zajął się problemem właściwej podstawy prawnej dla zawarcia umowy, a konkretniej pominięciem art. 16 ust. 2 TFUE. Trybunał przypomniał zasadnicze wymogi: wybór podstawy prawnej aktu UE, w tym aktu przyjętego w celu zawarcia umowy międzynarodowej, musi opierać się na obiektywnych czynnikach, które mogą zostać poddane kontroli sądowej, a do których należą w szczególności cel i treść tego aktu[38]. Oceniając cel i treść porozumienia, Trybunał – podobnie jak uczynił to rzecznik generalny P. Mengozzi w swojej opinii – doszedł do wniosku, że umowa zawiera dwa elementy składowe – pierwszy dotyczy konieczności zapewnienia bezpieczeństwa publicznego, a drugi – ochrony danych PNR. Tym samym, decyzja Rady w sprawie zawarcia umowy powinna opierać się zarówno na art. 16 ust. 2 TFUE, jak i na art. 87 ust. 2 lit. a TFUE, o ile procedura wynikająca z obu podstaw jest zgodna[39]. W tym konkretnym przypadku decyzja Rady w sprawie zawarcia przewidywanej umowy powinna – w ocenie Trybunału – opierać się łącznie na art. 16 ust. 2 TFUE i na art. 87 ust. 2 lit. a TFUE[40]. Przypomnieć przy tym należy, że wybór właściwej podstawy prawnej ma znaczenie konstytucyjne, ponieważ posiadając tylko kompetencje powierzone, UE musi powiązać przyjmowane akty z postanowieniem traktatu, które ją do tego przyjęcia skutecznie upoważniają, a zastosowanie błędnej podstawy prawnej może przesądzić o nieważności samego aktu zawarcia, a tym samym – o wadliwości zgody UE na związanie umową, którą podpisała. W tym konkretnym przypadku przywołanie właściwej podstawy prawnej nie miało znaczenia dla wyboru właściwej procedury – we wszystkich przypadkach zastosowanie znajduje zwykła procedura prawodawcza, natomiast wskazanie art. 16 ust. 2 TFUE jako podstawy powinno mieć znaczenie dla oceny celu umowy i jej priorytetów. Przyznanie pierwszeństwa podstawom z tytułu V części III TFUE wskazywałoby na przyznanie przewagi walorowi bezpieczeństwa, co mogłoby też rzutować na sposób interpretacji przepisów umowy[41]. Dobrze zatem, że Trybunał wyjaśnił tę kwestię w swojej opinii.

O wiele istotniejsze dla przyszłych porozumień i dla prawa ochrony danych osobowych w UE są te rozważania, w których Trybunał dokonał szczegółowej analizy umowy, zakończonej wnioskiem o jej niezgodności z art. 7, art. 8[42], art. 21 i art. 52 ust. 1

---

38 Opinia 1/2015, pkt 76. Zob. wyroki: z dnia 6 maja 2014 r., Komisja/Parlament i Rada, C-43/12, EU:C:2014:298, pkt 29; a także z dnia 14 czerwca 2016 r., Parlament/Rada, C-263/14, EU:C:2016:435, pkt 43 i przytoczone tam orzecznictwo.

39 Wyrok z dnia 6 listopada 2008 r. Parlament/Rada, C-155/07, EU:C:2008:605, pkt 37 i przytoczone tam orzecznictwo.

40 Pkt 105–118 opinii 1/15.

41 Autorka pisała o tych dylematach w kontekście RODO. Zob. A. Grzelak, *Główne cele ogólnego rozporządzenia o ochronie danych* [w:] M. Kawecki, T. Osiej, *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, Warszawa 2017, s. 11–25.

42 Należy przy tym zauważyć, że Trybunał ograniczył się wyłącznie do analizy art. 8 KPP, pomijając szczegółową analizę art. 16 ust. 1 TFUE i wskazując, że art. 8 KPP określa jednak bardziej szczegółowe wymagania, od jakich zależy dopuszczalność przetwarzania danych osobowych.

Karty Praw Podstawowych w zakresie, w jakim nie wyklucza przekazywania z Unii Europejskiej do Kanady danych szczególnie chronionych oraz wykorzystywania i zatrzymywania tych danych. Co do zasady Trybunał uznał, że przekazanie i przetwarzanie danych PNR, dotyczących zidentyfikowanych osób, narusza prawo podstawowe do ochrony prywatności (art. 7 KPP) oraz prawo do ochrony danych osobowych (art. 8 KPP). Istotą analizy jest jednak uzasadnienie tego naruszenia, w kontekście wymogów określonych w art. 8 ust. 2 oraz art. 52 ust. 1 KPP. Jednocześnie, w związku z tym, że celem umowy jest zapewnienie bezpieczeństwa publicznego poprzez przekazywanie danych PNR do Kanady i wykorzystywanie ich w ramach zwalczania przestępstw terrorystycznych i innych poważnych przestępstw, zatem ingerencja może być uzasadniona celem ogólnym UE. Ochrona bezpieczeństwa publicznego przyczynia się przecież do ochrony praw i wolności innych osób, a art. 6 KPP gwarantuje każdemu prawo nie tylko do wolności, ale też bezpieczeństwa osobistego[43]. Takie stwierdzenie Trybunału nie jest zaskakujące – było to już bowiem przedmiotem szerszych analiz, chociażby we wspomnianej wcześniej sprawie DRI.

Podstawowym problemem, jaki doprowadził do uznania niezgodności umowy z przepisami Karty było niespełnienie wymogu „konieczności" związanego z tym, że naruszenie musi być ograniczone wyłącznie do tego, co jest ściśle niezbędne. Trybunał zidentyfikował przy tym szereg problemów.

Po pierwsze, Trybunał stwierdził, że dane PNR, które miały być przekazywane, nie są wystarczająco jasno i precyzyjnie zdefiniowane. O ile 19 rubryk danych PNR, figurujących w załączniku do umowy, odpowiada zasadniczo wymogom wytycznych Organizacji Międzynarodowego Lotnictwa Cywilnego (ICAO), o tyle należy podkreślić, że są też takie, które wzbudzają wątpliwości. Wśród nich TSUE wskazał na „dostępne informacje dotyczące programów dla stałych klientów (*frequent flier*) i dotyczące korzyści (darmowe bilety, zamiana klasy biletu na wyższą itd.)" oraz „wszelkie dostępne informacje kontaktowe (w tym informacje na temat jednostki, która utworzyła dane)", bowiem one nie określają w sposób wystarczająco jasny i precyzyjny danych PNR podlegających przekazaniu[44]. W tym przypadku Trybunał uznał, że użyte sformułowania nie wyznaczają w sposób wystarczający zakresu danych podlegających przekazaniu. Warto przy tym nadmienić, że podobne sformułowania użyte w innych przypadkach (np. „wszelkie dostępne informacje o płatnościach") już takich zastrzeżeń nie budziły, bowiem ich interpretacja spełniała wymogi jasności i precyzji. Za nieprecyzyjne uznano też „uwagi ogólne, w tym inne informacje dodatkowe (OSI), informacje o usługach specjalnych (SSI) i o prośbach o usługi specjalne (SSR)". Przy tym te dane uznane zostały za potencjalnie ujawniające dane sensytywne, które mogłyby być przetwarzane w sposób sprzeczny z art. 21 KPP (zakaz dyskryminacji), a tym samym legalność ich przetwarzania wymagałaby precyzyjnego i szczególnie solidnego uzasadnienia,

[43] Pkt 148–151 opinii 1/15.
[44] Pkt 156 opinii 1/15.

opartego na przesłankach innych niż ochrona porządku publicznego, czego w tym przypadku zabrakło[45].

Po drugie, TS przyjrzał się kwestii zautomatyzowanego przetwarzania danych PNR. Dane PNR przekazywane do Kanady powinny być zasadniczo analizowane w sposób zautomatyzowany, a tymczasem ocena ryzyka stwarzanego przez pasażerów lotniczych dla bezpieczeństwa ruchu lotniczego jest przeprowadzana przed przybyciem pasażerów do Kanady, co naturalnie może być obarczone błędem. Zatem każdy wynik pozytywny powinien być poddany indywidualnej ocenie przeprowadzanej w sposób niezautomatyzowany[46].

Trzeci analizowany problem dotyczył celów przetwarzania danych. Zdefiniowanie pojęć „przestępstwo terrorystyczne" czy „poważne przestępstwo międzynarodowe" uznane zostało przez TS za wystarczające[47]. Trybunał uznał jednak, że umożliwienie przetwarzania danych „w poszczególnych przypadkach" w celach, odpowiednio, „zapewnienia nadzoru nad administracją publiczną lub jej odpowiedzialności" oraz „dostosowania się do wydanego wezwania do stawiennictwa w sądzie lub też nakazu lub zarządzenia wydanego przez sąd" nie spełnia wymogów jasności i precyzji[48].

Czwarty problem dostrzeżony przez Trybunał dotyczył zatrzymania i wykorzystywania danych PNR. Trybunał przypomniał warunki, na jakich organy kanadyjskie mogą mieć dostęp do danych i je zatrzymywać, podkreślając, że uregulowania muszą spełniać obiektywne kryteria ustanawiające związek między danymi osobowymi podlegającymi zatrzymaniu a zamierzonym celem[49]. Cele te umowa określa w art. 3, a Trybunał przeanalizował je w kontekście różnych momentów przetwarzania danych. Uznał, że w przypadku zatrzymywania danych PNR i ich wykorzystywania do chwili opuszczenia Kanady przez pasażerów lotniczych oraz podczas pobytu pasażerów lotniczych w Kanadzie, zatrzymanie i wykorzystanie danych może być uzasadnione i nie wykracza poza granice tego, co ściśle konieczne, bowiem może pojawić się konieczność wykorzystania danych w celu zwalczania terroryzmu i poważnych przestępstw międzynarodowych. Jednak w przypadku danych wpuszczonych już do Kanady, przetwarzanie danych PNR powinno opierać się na innych okolicznościach uzasadniających ich wykorzystanie, przy czym oczywiście potrzeba zwalczania terroryzmu i poważnych przestępstw może to uzasadniać. W takich przypadkach jednak co do zasady przetwarzanie danych powinno być uzależnione od uprzedniej kontroli dokonywanej bądź przez sąd bądź przez inny niezależny organ administracyjny[50]. Jednak w sytuacji, w której pasażerowie opuścili terytorium Kanady należy przyjąć, że nie stanowią już zagrożenia w zakresie terroryzmu lub poważnych przestępstw międzynarodowych, skoro ani kontrole graniczne przy wjeździe i opuszczeniu kraju, ani też inne weryfikacje podczas

45 Pkt 165 opinii 1/15.
46 Pkt 168–174 opinii 1/15.
47 Pkt 175–178 opinii 1/15.
48 Pkt 179–181 opinii 1/15.
49 Tu TS odwołał się w szczególności do wyroków w sprawie *Schrems I* oraz w sprawie *Tele2 Sverige i Watson*.
50 Pkt 202 opinii 1/15.

pobytu nie wykazały obiektywnych przyczyn do dalszego przetwarzania danych. Zatem w takim przypadku, nie istnieje chociażby pośredni związek między danymi PNR osób, które opuściły terytorium Kanady, a celem umowy. Co do zasady zatem, trwałe przechowywanie danych PNR ogółu pasażerów lotniczych po opuszczeniu przez nich Kanady nie może zostać uznane za konieczne. Jednak może się okazać, że w indywidualnych przypadkach osoby, które wyjeżdżają, takie zagrożenie stwarzają, i wówczas przetwarzanie danych może być uzasadnione, przy czym – znów – powinno podlegać uprzedniej kontroli sądu lub niezależnego organu administracyjnego.

Piąty problem zdefiniowany w opinii 1/15 dotyczył udostępniania danych. Trybunał Sprawiedliwości nie zgodził się, by dane były przekazywane przez organy kanadyjskie władzom państw trzecich, co do których poziom ochrony zapewnianej w tych państwach byłby oceniany przez organy kanadyjskie. Przypomniał w szczególności wymogi wynikające z orzeczenia w sprawie *Schrems I*: przekazywanie danych osobowych z UE do państwa trzeciego może mieć miejsce wyłącznie wówczas, gdy państwo to zapewnia poziom ochrony podstawowych praw i wolności zasadniczo równoważny poziomowi gwarantowanemu w UE. Ten sam wymóg dotyczy przypadków udostępniania danych PNR z Kanady do innych państw trzecich – tak, by nie obchodzić wymogów wynikających z prawa UE. By możliwe było przekazanie danych PNR do państwa trzeciego, konieczne byłoby zawarcie umowy między UE a państwem trzecim albo decyzji Komisji, przyjętej na podstawie stosownych przepisów (w ówczesnym stanie prawnym TSUE wskazał na art. 25 ust. 6 dyrektywy 95/46/WE)[51]. Podobnie, umowa nie określała żadnych szczegółów, które pozwoliłyby uznać, że udostępnianie danych podmiotom prywatnym będzie dopuszczalne (ani kręgu beneficjentów, ani sposobu, w jaki informacje mogłyby zostać wykorzystane), w tym nie wymagała, by udostępnienie danych PNR pozostawało w związku z celem umowy.

Trybunał podniósł także inne zastrzeżenia, w tym wskazał na brak obowiązku notyfikacji podmiotu danych o ich wykorzystaniu lub udostępnieniu na warunkach wynikających z umowy[52]. Wreszcie przypomniał znaczenie niezależnego nadzoru nad przestrzeganiem zasad przetwarzania danych i uznał, że dopuszczenie, by nadzór sprawował nie tylko „niezależny organ publiczny", lecz również „inny organ ustanowiony środkami administracyjnymi (…), który sprawuje swoją funkcję w sposób bezstronny i działa w sposób niezależny, co można potwierdzić". Takie sformułowanie, w ocenie TSUE, budzi wątpliwości, czy faktycznie taki organ nie będzie podporządkowany innemu, który może wpływać na jego decyzje[53].

[51] Pkt 212–215 opinii 1/15.
[52] Pkt 221–225 opinii 1/15.
[53] Pkt 228–231 opinii 1/15.

5. Konsekwencje opinii 1/15 dla systemu PNR i ochrony danych osobowych w Unii Europejskiej

5.1. Przede wszystkim należy stwierdzić, że stanowisko Trybunału nie było zaskakujące. Trybunał Sprawiedliwości w dużej mierze oparł się na swoich wcześniejszych orzeczeniach, w tym na wspomnianych już ustaleniach w sprawach DRI czy *Schrems I*. Nie odszedł od swojego stanowiska, chociaż niektóre państwa członkowskie w trakcie postępowania argumentowały (do czego szerzej odniósł się w swojej opinii rzecznik generalny), że instytucje powinny mieć dalej idące uprawnienia, a standard ochrony powinien być nieco niższy w przypadku aktów wchodzących w zakres relacji zewnętrznych. Trybunał zastosował identyczną miarę wobec zarówno umów międzynarodowych zawieranych przez UE, jak i aktów skierowanych do wewnątrz UE.

Słusznie zauważają Martyna Kusak i Paweł Wiliński[54], że Trybunał wskazał wyraźnie, że stosowanie środków polegających na nieukierunkowanym i nieograniczonym gromadzeniu danych jest nieproporcjonalną ingerencją w prawa podstawowe, a w efekcie jest niezgodne z prawem UE. Marcin Rojszczak zauważa, że wniosek ten jest aktualny wobec każdego działania, którego skutkiem jest zatrzymywanie danych, zatem dotyczy również metadanych[55], a także działań organów zajmujących się bezpieczeństwem publicznym. Trzeba jednak pamiętać, że zarówno opinia 1/15, jak i późniejsze orzecznictwo TS dowodzi, że dzieje się tak wyłącznie wówczas, gdy nie jest wykazana konieczność i proporcjonalność działań, wyrażające się w realizacji wymogów określonych w tych orzeczeniach. Trybunał ustanowił bardzo wysoki standard ochrony danych osobowych[56].

To z kolei może budzić wątpliwości podniesione przez niektórych ekspertów, którzy postawili pytanie, czy takie rygorystyczne stanowisko nie doprowadzi do trudności w negocjacjach z państwami trzecimi, które mając wiedzę o tym, że wynegocjowana umowa może zostać zakwestionowana następczo przez Trybunał, nie będą chciały podejmować takich wysiłków i inwestować swojego czasu i energii w negocjacje[57]. To z kolei otwiera dyskusję w sprawie w ogóle zasadności wypowiadania się przez TSUE odnośnie do umów, które nie weszły jeszcze w życie – przy czym należy przychylić się do stanowiska Mario Mendeza, który zasadnie wskazuje, że przecież właśnie ten

---

[54] M. Kusak, P. Wiliński, *Ochrona danych osobowych w ściganiu przestępstw. Standardy krajowe i unijne*, Warszawa 2020, s. 89 i n.

[55] M. Rojszczak, *Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*, Warszawa 2019, s. 476–477.

[56] W. Wiewiórowski, *Surveillance for public security purposes. Four pillars of acceptable interference with the fundamental right to privacy* [w:] *Data Protection and Privacy under Pressure*, red. G. Vemueulen, E. Lievens, Maklu 2017, s. 185–189.

[57] Ch. Kuner, *Data Protection, Data Transfers, and International Agreements: the CJEU's Opinion 1/15*, Verfassungsblog, 26 July 2017, verfassungsblog.de [dostęp: 25.11.2021]. Autor wskazuje m.in. że zarówno rzecznik generalny, jak i TSUE dokonali bardzo szczegółowej analizy umowy, kwestionując m.in. użycie skrótu „itd." w załączniku określającym wykaz przetwarzanych danych (zob. pkt 157 wyroku). Autor podkreśla również, że TSUE nie wyjaśnił dokładnie, na jakich źródłach opierał się, oceniając umowę.

moment umożliwia zapobieżenie wejściu w życie umowy, która nie spełnia podstawowych wymogów odnośnie do zgodności z traktatami[58]. Hielke Hijmans uważa, że Trybunał wręcz przejął rolę współprawodawcy – fakt, że Trybunał dokonał bardzo dogłębnej analizy porozumienia pozwala uzasadnić takie stanowisko, chociaż oczywiście, zgodnie z art. 218 ust. 11 TFUE, Trybunał Sprawiedliwości jest uprawniony do kontrolowania wynegocjowanej już umowy[59]. Bez wątpienia jednak takie podejście Trybunału może utrudniać jakiekolwiek dalsze rozmowy i negocjacje, powodując, że negocjatorzy unijni mają związane ręce.

5.2. W opinii 1/15 Trybunał Sprawiedliwości nie zakwestionował w ogóle systemu PNR, uznając go za potrzebny i przydatny do zwalczania terroryzmu i poważnej przestępczości. Trybunał zasadniczo zgodził się ze stanowiskiem, że zatrzymywanie danych PNR i ich wykorzystywanie do chwili opuszczenia Kanady przez pasażerów lotniczych jest co do zasady dopuszczalne, bowiem pozwala na ułatwienie kontroli bezpieczeństwa i kontroli granicznych. Zatrzymywanie i wykorzystywanie danych PNR w tym celu z samej swej istoty nie może być ograniczone do określonego kręgu pasażerów lotniczych, ani podlegać uprzedniej zgodzie sądu lub niezależnego organu administracyjnego. Tymczasem w sprawie *Tele2/Watson* Trybunał uznał, że niedopuszczalna jest uogólniona i niezróżnicowana retencja danych. W opinii 1/15 Trybunał nie wyjaśnił, czym różni się retencja danych PNR od tych, o których mowa w sprawie *Tele2/Watson* – można jedynie domyślać się tak, jak czyni to Lorna Woods, że chodzi o charakter danych[60.] Trybunał stwierdził jedynie, że przetwarzanie danych w ramach umowy było ograniczone wyłącznie do niektórych aspektów życia prywatnego, „w szczególności dotyczących podróży lotniczych między Kanadą a Unią Europejską"[61.].W istocie, można było oczekiwać od Trybunału bardziej dokładnego wyjaśnienia i wskazania tych elementów, które ukazywałyby niezbędność i proporcjonalność masowego i rutynowego przetwarzania danych osób, które zasadniczo nie są o nic podejrzewane, do celów walki z przestępczością[62]. Tym samym, Trybunał zaakceptował co do zasady przetwarzanie danych PNR, o ile spełnione zostaną warunki i ograniczenia wskazane w opinii 1/15, przy czym szczególnie jest to istotne w kontekście tych przepisów, które miałyby zezwalać na przekazywanie danych PNR do państw trzecich[63].

---

58 M. Mendez, *Opinion 1/15: The Court of Justice Meets PNR Data (Again!)*, „European Papers" 2017, vol. 2, nr 3, s. 812. Zob. również *idem*, *Constitutional Review of Treaties: Lessons for Comparative Constitutional Design and Practice*, „International Journal of Constitutional Law" 2017, p. 84.

59 H. Hijmans, *PNR Agreement EU-Canada*…, s. 410.

60 L. Woods, *Transferring Personal Data Outside the EU: Clarification from the ECJ?*, EU Law Analysis, 4 August 2017, eulawanalysis.blogspot.co.uk [dostęp: 25.11.2021].

61 Pkt 150 opinii 1/15.

62 Tak w swojej opinii wskazywał m.in. EDPS. Zob. cytowaną już opinię 5/2015 z 24.09.2015 r. w sprawie umowy z Kanadą.

63 Na to zwraca uwagę Ch. Kuner, *Court of Justice International agreements, data protection, and EU fundamental rights on the international stage: Opinion 1/15, EU-Canada PNR*, „Common Market Law Review" 2018, vol. 55, nr 3, s. 857–882.

5.3. Dla samej umowy z Kanadą opinia 1/15 Trybunału Sprawiedliwości miała fundamentalne znaczenie, bowiem – zanim mogłaby zostać zawarta – musiałaby zostać istotnie zmieniona. To zaś oznacza otwarcie negocjacji na nowo. Zgodnie z art. 218 ust. 11 TFUE, w przypadku negatywnej opinii Trybunału przewidywana umowa nie może wejść w życie, chyba że nastąpi jej zmiana lub rewizja Traktatów. Do rewizji traktatów nie dojdzie w tym względzie oczywiście, zatem konieczne było podjęcie dalszych negocjacji. Jeszcze w 2017 r. Komisja przesłała Radzie zalecenie dotyczące rozpoczęcia negocjacji[64], które zainicjowano w czerwcu 2018 r. W lipcu 2019 r. zarówno UE, jak i Kanada we wspólnym oświadczeniu wypowiedziały się w sprawie konieczności szybkiego sfinalizowania prac nad umową[65]. Taka umowa, której treści do dnia dzisiejszego nie znamy, mogłaby stanowić swoisty wzór – modelowe rozwiązanie dla przyszłych umów z państwami trzecimi. W negocjowanych umowach z Japonią czy Meksykiem, ewentualnie z innymi państwami trzecimi, szczególnie rygorystycznie powinno podejść się do problemu konieczności i proporcjonalności systemu PNR, a także do praktycznego wdrażania zasady celowości dotyczącej wykorzystywania przekazanych danych PNR.

5.4. Większy problem dotyczy tego, jak opinia 1/15 wpływa na obowiązujące umowy z USA i Australią. Pomijając problem podstawy prawnej (porozumienia zostały zawarte na tej samej podstawie prawnej, którą zakwestionował TSUE w opinii 1/15), należy stwierdzić, że to obydwie umowy zawierają merytoryczne rozwiązania równoważne tym, które TSUE podniósł jako niezgodne z KPP i TFUE w opinii dotyczącej umowy z Kanadą[66]. Umowy te zawarte były w stanie prawnym poprzedzającym wyrok TSUE w sprawach *DRI* czy *Tele 2/Watson*.

Do najważniejszych problemów występujących w obu umowach zaliczyć należy ten sam zakres danych (nieprecyzyjny), jak w przypadku Kanady, a także niedopuszczalność przekazywania danych sensytywnych bez wyraźnego i bardzo dokładnego uzasadnienia. W obu porozumieniach występują problemy dotyczące zasady celowości, zwłaszcza że w przypadku umowy z USA chodzi nie tylko o przestępczość terrorystyczną, ale również o wiele szerzej – o „przestępstwa powiązane" (*related crimes*), zaś „przestępstwa transgraniczne" są bardzo szeroko zdefiniowane. Dane PNR, o ile zajdzie konieczność, mogą być wykorzystywane i przetwarzane w indywidualnych przypadkach, gdy jest to niezbędne z uwagi na poważne zagrożenie, oraz w celu ochrony żywotnych interesów jakiejkolwiek osoby fizycznej, lub jeżeli nakaże tak sąd (art. 4 ust. 2 umowy z USA). Departament Bezpieczeństwa Wewnętrznego USA może także wykorzystywać i przetwarzać dane PNR w celu identyfikacji osób, które po przyjeździe do Stanów Zjednoczonych lub przed opuszczeniem tego państwa zostałyby

[64] Komisja Europejska, Zalecenie w sprawie decyzji Rady upoważniającej do rozpoczęcia negocjacji w sprawie Umowy między Unią Europejską a Kanadą o przekazywaniu i wykorzystywaniu danych dotyczących przelotu pasażera (PNR) w celu zapobiegania terroryzmowi i innym poważnym przestępstwom o charakterze międzynarodowym oraz walki z nimi, COM(2017) 605 final.

[65] Zob. pkt 11 Canada – EU Summit Joint Declaration, July 17–18, 2019, Montreal, https://www.consilium.europa.eu/media/40403/final-2019-joint-declaration-final.pdf [dostęp: 25.11.2021].

[66] Analizy dokonał M. Mendez, *Opinion 1/15*…, s. 815–818.

poddane dokładniejszemu przesłuchaniu lub sprawdzeniu, lub w przypadku których może zachodzić konieczność dalszego sprawdzenia (art. 4 ust. 3 umowy z USA)[67]. Żadna z umów nie dokonuje rozróżnienia między danymi osób, które przybyły już i przebywają na terytorium państwa trzeciego i osób, które z niego wyjechały. Obie umowy przewidują również przekazywanie danych PNR do państw trzecich – co zgodnie z opinią 1/15 – wymagałoby porozumienia między UE a państwem trzecim lub decyzji o adekwatności poziomu ochrony.

Jasno zatem widać, że obie umowy nie są zgodne z KPP oraz TFUE w podobnym zakresie, w jakim za niezgodną uznał TSUE umowę z Kanadą. Jednak obie umowy obowiązują i nie ma obecnie prawnej możliwości ich unieważnienia w trybie określonym w art. 218 czy art. 263 TFUE. Otwarte pozostaje pytanie, czy takiej oceny ważności nie mógłby dokonać Trybunał Sprawiedliwości w odpowiedzi na pytanie prejudycjalne sądu krajowego[68]. Umowa z USA, która weszła w życie w 2012 r., zgodnie z art. 26 pozostaje w mocy przez okres siedmiu lat od dnia jej wejścia w życie, a po upływie tego termin i wszelkich kolejnych okresów – jest przedłużana na okres kolejnych siedmiu lat, o ile jedna ze stron nie powiadomi drugiej strony drogą dyplomatyczną, z co najmniej dwunastomiesięcznym wyprzedzeniem, o zamiarze nieprzedłużania umowy. Takiego zamiaru dotychczas nie wyrażono, a Komisja nie podjęła działań zmierzających do renegocjacji umowy, co według M. Mendeza, mogłoby być nawet podstawą do wszczęcia postępowania przeciwko Komisji (skarga na bezczynność) na podstawie art. 265 TFUE[69], skoro Komisja ma świadomość niezgodności postanowień obu umów z traktatami i KPP. Rówież Christopher Kuner stawia pytania o działania instytucji UE, zastanawiając się, jak to jest możliwe że Komisja i Rada wynegocjowały i zaakceptowały tekst, który następnie został uznany przez TS za posiadający tak istotne wady, jeśli chodzi o poziom ochrony praw podstawowych. Christopher Kuner przypomina przy tym, że przecież Kanada ma długą historię współpracy z UE w dziedzinie ochrony danych osobowych, i że prawo tego państwa jest stosunkowo bliskie rozwiązaniom unijnym – jak w tym świetle przedstawia się możliwość wynegocjowania satysfakcjonującego tekstu z państwami charakteryzującymi się o wiele niższym standardem ochrony?[70]

5.5. Wreszcie, opinia 1/15 powinna mieć znaczenie dla systemu EU-PNR, prowadząc nie tylko do zmian w jego funkcjonowaniu, ale przede wszystkim w regulacjach[71].

---

[67] Zob. również art. 4 ust. 3 umowy między Stanami Zjednoczonymi Ameryki a Unią Europejską o wykorzystywaniu danych dotyczących przelotu pasażera oraz przekazywaniu takich danych do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych (Dz. Urz. L 215 z 2012 r., s. 5).

[68] Takiej oceny dokonywał TSUE w odpowiedzi na pytania prejudycjalne sądu krajowego w odniesieniu do ważności porozumienia o partnerstwie w sektorze rybołówstwa pomiędzy Wspólnotą Europejską a Królestwem Marokańskim (Dz. Urz. L 141 z 2006 r., s. 4). Zob. wyrok TSUE w sprawie C-266/16 *Western Sahara Campaign UK*, z dnia 27 lutego 2018 r., ECLI:EU:C:2018:118.

[69] M. Mendez, *Opinion 1/15*…, s. 816.

[70] Ch. Kuner, *Court*…, s. 857–882.

[71] Geneza i przyczyny przyjęcia dyrektywy 2016/681 – zob. D. Lowe, *The European Union's Passenger Name Record Data Directive 2016/681: Is It Fit for Purpose?*, „International Criminal Law Review" 2016,

Chociaż Komisja Europejska w chwili obecnej takiej potrzeby nie dostrzega[72], to jednak wątpliwości może wzbudzać w szczególności zakres gromadzonych danych (w tym przede wszystkim „uwagi ogólne")[73]. Ostateczna ocena co do tego, czy ograniczenia praw podstawowych określonych w dyrektywie EU-PNR są dopuszczalne, wymaga analizy pod kątem konieczności i proporcjonalności. W szczególności, brak jakiejkolwiek wzmianki o ochronie praw podstawowych w dyrektywie EU-PNR może budzić obawy co do jej rzeczywistego wpływu na prawa podstawowe i stawiać pod znakiem zapytania kwestię, czy taki program jest rzeczywiście niezbędny do skutecznego zwalczania poważnej przestępczości oraz terroryzmu, chociaż oczywiście fakt, że walka z międzynarodowym terroryzmem i utrzymanie międzynarodowego pokoju i bezpieczeństwa, a także zapewnienia bezpieczeństwa publicznego stanowi cel interesu ogólnego wynika z dotychczasowego orzecznictwa[74]. W literaturze podkreśla się też, że wątpliwości może budzić kwestia celowości (art. 7 ust. 5 dyrektywy EU-PNR), zakres gromadzonych danych, okres zatrzymania danych, nieprecyzyjne gwarancje procesowe i wreszcie przyznanie prawa do porównywania danych PNR z danymi zgromadzonymi w bazach prowadzonych do innych celów[75]. Ta ostatnia kwestia była podnoszona przez Europejskiego Inspektora Ochrony Danych, który – w przypadku umowy z Kanadą – krytykował regulowane porównywanie danych PNR z nieograniczoną liczbą niezdefiniowanych baz, uznając, że jest to nadmierne i nieproporcjonalne[76]. Dyrektywa musi ustanawiać jasne i precyzyjne reguły co do zakresu i stosowania transferu danych oraz regulować minimalne zabezpieczenia i gwarancje skutecznej

---

nr 16, s. 856–884. Autor uważa, że dyrektywa dobrze realizuje założenia prawa do prywatności i nie wzbudza większych zastrzeżeń. W świetle pytań prejudycjalnych skierowanych przez sądy krajowe do TSUE takie stanowisko może jednak się nie utrzymać. Innego zdania jest zdecydowanie S. Roda, która przedstawia swoją analizę, z której wynika, że część przepisów dyrektywy wymaga zmiany. Zob. *eadem*, *Shortcomings of the Passenger Name Record Directive in Light of Opinion 1/15 of the Court of Justice of the European Union*, „European Data Protection Law Review" 2020, nr 1, s. 66 i n. Zob. też S. Fantin, P. Vogiatzoglou, P. Dewitte, K. Quezada Tavárez, *From Theory To Practice: Exercising The Right Of Access Under The Law Enforcement And PNR Directives*, „Journal of Intellectual Property" 2020 nr 11, https://ssrn.com/abstract=3777074 [dostęp: 25.11.2021]. Z kolei wątpliwości co do uregulowania kwestii profilowania w dyrektywie EU PNR wyrażali również V. Papakonstantinou, P. De Hert, *Repeating the Mistakes of the Past Will Do Little Good for Air Passengers in the EU: The Comeback of the EU PNR Directive and a Lawyer's Duty to Regulate Profiling*, „New Journal of European Criminal Law", 2015 nr 2, s. 160, ale także np. J. Wojnowska-Radzińska, która wyjaśnia też założenia dyrektywy, zob. *eadem*, *Legitimizing Pre-Emptive Data Surveillance under EU Law – the case of the PNR Directive*, RPEiS 2021, z. 1, https://doi.org/10.14746/rpeis.2021.83.1.9. [dostęp: 25.11.2021].

[72] Zob. wnioski płynące ze sprawozdania zawartego w sprawozdaniu COM(2020) 305 final.

[73] Autorka niniejszego opracowania również przedstawiała wątpliwości na etapie prac nad projektem dyrektywy. Zob. w szczególności: A. Grzelak, *Opinia dotycząca projektu dyrektywy Parlamentu Europejskiego i Rady w sprawie wykorzystania danych dotyczących przelotu pasażera w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich ścigania*, „Zeszyty Prawnicze Biura Analiz Sejmowych" 2011, nr 2, s. 39–52.

[74] Zob. w szczególności wyrok w sprawie *Kadi*, ECLI:EU:C:2008:461, pkt 363; *Al-Aqsa* (ECLI:EU:C:2012:711), pkt 130); *Tsakouridis* (ECLI:EU:C:2010:708), pkt 46 i 47.

[75] S. Roda, *Shortcomings of the Passenger Name Record Directive*…, s. 77–78.

[76] Opinia EIOD 5/2015 z 24.09.2013, pkt 37.

ochrony danych osobowych przed ryzykiem nadużycia oraz przed wszelkim niezgodnym z prawem dostępem i wykorzystaniem tych danych. Oceny tego, czy tak rzeczywiście jest, może dokonać Trybunał Sprawiedliwości, jednak dotychczasowa wykładnia art. 7, art. 8 i art. 52 ust. 1 Karty oraz art. 16 TFUE może prowadzić do oczekiwania, że dyrektywa EU-PNR powinna zostać zmieniona.

Trzeba przy tym zauważyć, że w chwili obecnej trwają analizy zgodności dyrektywy EU-PNR z wymogami wynikającymi z traktatu i KPP, bowiem w trybie art. 267 TFUE, przed Trybunałem zawisło kilka postępowań, w których sądy krajowe proszą o ocenę ważności dyrektywy lub o wykładnię jej przepisów:

1) C-486/20 – pytanie sądu słoweńskiego z 1.10.2020 r. w sprawie *Varuh človekovih pravic Republike Slovenije (Rzecznik Praw Obywatelskich Słowenii)* – dotyczy pkt 8 i pkt 12 załącznika do dyrektywy 2016/681 i oceny zgodności z art. 7 i art. 8 oraz z art. 52 ust. 1 KPP;
2) C-222/20 – pytanie z 27.05.2020 r. niemieckiego Verwaltungsgericht Wiesbaden w sprawie *OC / Bundesrepublik Deutschland* – sąd krajowy sformułował kilka pytań, dotyczących przede wszystkim wykładni art. 7 i art. 8 KPP w związku z krajowymi przepisami wdrażającymi dyrektywę 2016/681;
3) C-215/20 – pytanie z 19.05.2020 r. niemieckiego Verwaltungsgericht Wiesbaden, który sformułował bardzo ważne pytanie ogólne plus pytania szczegółowe, zmierzające do ustalenia, czy dyrektywa 2016/681 jest zgodna z art. 7, art. 8 i art. 52 Karty;
4) trzy sprawy z identycznymi pytaniami:
   a) C-148/20 – pytanie z 16.03.2020 r. sądu niemieckiego w sprawie *AC / Deutsche Lufthansa AG*;
   b) C-149/20 – pytanie z 16.03.2020 r. sądu niemieckiego w sprawie *DF / Deutsche Lufthansa AG*;
   c) C-150/20 – pytanie z 17.03.2020 r. sądu niemieckiego w sprawie *BD / Deutsche Lufthansa AG*.
5) C-817/19 – pytanie z 31.10.2019 r. belgijskiego Cour constitutionnelle (Belgia) w sprawie *Ligue des droits humains / Conseil des ministers* – w tym przypadku, poza pytaniami dotyczącymi samej dyrektywy 2016/681, jest również pytanie odnoszące się do zakresu stosowania RODO w kontekście przepisów krajowych wdrażających dyrektywę.

Wszystkie te sprawy są w toku i w żadnej nie przedstawiono jeszcze opinii rzecznika generalnego.

5.6. Problem wyważenia między prawem do prywatności a porządkiem publicznym i bezpieczeństwem pojawił się również we wspomnianych już sprawach *Privacy International* oraz *La Quadrature du Net i in.*[77] Trybunał Sprawiedliwości w tych sprawach

[77] Wyroki te wymienione zostały w przypisie 5. Na temat tych wyroków zob. też A. Grzelak, K. Zielińska, *Między prawem do prywatności i ochrony danych osobowych a zapewnieniem bezpieczeństwa publicznego i walką z przestępczością. Problemu retencji danych ciąg dalszy – glosa do wyroków Trybunału*

analizował możliwość zastosowania dyrektywy o e-prywatności do działalności związanej z bezpieczeństwem narodowym i zwalczaniem terroryzmu, a także zakres, w jakim państwa członkowskie mogą dokonać ograniczenia prawa do prywatności i ochrony danych osobowych dla celów związanych z bezpieczeństwem narodowym i zwalczaniem terroryzmu. Trybunał dokonał też analizy art. 6 Karty, ponieważ jest wykorzystywany jako argument przez państwa członkowskie do uzasadnienia ingerencji w prawo do prywatności. Wyroki i opinie rzeczników generalnych w tych sprawach są bardzo obszerne, jednak niektóre wnioski można odnieść również do systemu PNR, bowiem w sprawie *Privacy International* głównym problemem było masowe gromadzenie danych i zautomatyzowane przetwarzanie w celu ochrony bezpieczeństwa narodowego przez krajowe agencje wywiadowcze, z kolei w sprawie *La Quadrature du Net* Trybunał analizował uogólnione i niedyskryminacyjne zatrzymywanie danych oraz legalność procedur retencji danych (problem powiadamiania podmiotu danych), a także rozważał, czy poza uzasadnieniem, jakim jest walka z bezpieczeństwem narodowym, zwalczaniem terroryzmu i poważnej przestępczości, również bezpieczeństwo terytorium, porządek publiczny i inne podobne argumenty uzasadniają dopuszczalność przetwarzania danych, i czy taki obowiązek nie wynika przy okazji z art. 4 i 6 KPP. I chociaż dotyczą one bardziej relacji wewnętrznych UE, i w tym aspekcie stanowisko TS jest nieco bardziej zniuansowane, to jednak zasadnicze poglądy wyrażane w wyrokach DRI i późniejszych zostało utrzymane.

5.7. Na poziomie ogólniejszym można zastanawiać się nad istotą prawa do ochrony prywatności i prawa do ochrony danych osobowych. Christopher Kuner zauważa, że w ostatnich latach TS kilkakrotnie wypowiadał się na ten temat, wskazując, iż – po pierwsze – masowa retencja danych nie wpływa na istotę prawa do prywatności zgodnie z art. 7 KPP, bowiem nie prowadzi do wyjawienia treści komunikacji elektronicznej[78]; po drugie – nie narusza istoty prawa do ochrony danych osobowych określonego w art. 8 KPP, bowiem dostawcy usług muszą przestrzegać stosownych przepisów[79]; po trzecie – przyjęte rozwiązania prawne są wyrazem kompromisu wobec treści art. 7 KPP[80]; i wreszcie – gwarantuje prawa osobom, których dane są przetwarzane, w tym prawo dostępu[81]. W opinii 1/15 TSUE również nie uznał, by doszło do naruszenia istoty prawa do prywatności i prawa do ochrony danych osobowych, bowiem przekazywane dane były ograniczone wyłącznie do pewnego wycinka prywatności, związanej z podróżami lotniczymi. Słusznie wskazuje Christopher Kuner, że potrzeba jasności i przewidywalność sprawia, iż ważne jest opracowanie ram normatywnych – do tej pory Trybunał nie chciał się wypowiedzieć na temat samych kryteriów, co byłoby istotne zwłaszcza ze względu na to, że sama prywatność jest pojmowana kontekstowo i defi-

---

Sprawiedliwości z 6.10.2020 r.: C-623/17, Privacy International, oraz w sprawach połączonych C-511/18, C-512/18, C-520/18, La Quadrature du Net i in., EPS 2021, nr 8, s. 28.

78 Wyrok ws. DRI, pkt 39.

79 *Ibidem*, pkt 40.

80 Wyrok ws. *Schrems I*, pkt 94.

81 *Ibidem*, pkt 95.

niowana na podstawie indywidualnych przypadków. Być może, jak uważa Maja Brkan, nie ma po prostu możliwości określenia abstrakcyjnie tego, co stanowi istotę praw podstawowych[82]. Być może w istocie tak jest, ale jednak z orzecznictwa TS wynika, że naruszenie istoty prawa podstawowego jest nielegalne i nie jest przedmiotem testu proporcjonalności, co wiązałoby się z koniecznością podjęcia próby zdefiniowania tego pojęcia.

6. Wnioski

Opinia 1/15 jest wyrazem troski Trybunału o wysoki standard ochrony prywatności i danych osobowych i stanowi kontynuację stanowiska wyrażanego w sprawach DRI, *Schrems I*, *Tele2/Watson* czy *Schrems II*. Trybunał po raz kolejny udowodnił, że nie pozwoli na obchodzenie i obniżanie standardów w relacjach zewnętrznych, w tym w zawieranych przez UE umowach bilateralnych. Pozostaje otwartą kwestia, czy Komisja Europejska będzie w stanie i czy będzie próbować przekonać państwa trzecie o konieczności przestrzegania wymogów wynikających z opinii 1/15. Pewne wątpliwości budzi fakt, że problem ten nie stał się jeszcze przedmiotem rozmów z USA i Australią, zaś dyrektywa 2016/681 w ocenie Komisji nie wymaga zmian.

Ostatecznie Trybunał nie odrzucił systemu PNR w całości, tworząc jednak tzw. checklistę wymogów proceduralnych, które muszą być spełnione, by uznać dopuszczalność stosowania tych rozwiązań. Spełnienie wymogów wskazanych przez Trybunał jest trudne, co – biorąc pod uwagę, jak spowolnione zostały rozmowy w sprawie systemów PNR – oznacza, że w praktyce kontynuowanie umów jest bardzo utrudnione[83]. I chociaż – patrząc przez pryzmat praw podstawowych – można zarzucać Trybunałowi, że opowiedział się za dopuszczalnością uogólnionego i niedyskryminacyjnego systemu inwigilacji podróżujących, to jednak w istocie Trybunał zmiękczył bardzo swoje stanowisko, wprowadzając liczne wymogi proceduralne, które mają chronić prawa podstawowe[84].

Trybunał w opinii 1/15 przedstawił wyważone stanowisko, ponieważ nie posunął się za daleko i zasadniczo dał zielone światło systemom PNR. Jednakże Trybunał tak szczegółowo zbadał istotę umowy, że może to mieć i zapewne ma kłopotliwe konsekwencje dla stosunków międzynarodowych UE. Nie wiadomo jeszcze, czy Komisja będzie w stanie przekonać państwa trzecie o konieczności spełnienia wysokich

---

[82] M. Brkan, *In Search of the Concept of Essence of EU Fundamental Rights Through the Prism of Data Privacy*, „Maastricht Faculty of Law Working Paper" 2017 nr 1, 16.01.2017. *Eadem*, *The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning*, „German Law Journal" 2019, nr 20, s. 864–883.

[83] E. Guild, E. Mendos Kuşkonmaz, *EU Exclusive jurisdiction on surveillance related to terrorism and serious transnational crime: case review on Opinion 1/15*, „European Law Review" 2018, vol. 43, nr 4, s. 583–597.

[84] A. Vedaschi, *The European Court of Justice on the EU-Canada Passenger Name Record Agreement*, „European Constitutional Law Review" 2018, vol. 14, nr 2, s. 410–429.

standardów określonych w opinii 1/15, przy czym Stany Zjednoczone są bez wątpienia najtrudniejsze do przekonania, biorąc pod uwagę ich rozbieżne podejście do prywatności. W każdym razie pozostaje jeszcze do odrobienia lekcja związana z koniecznością zmiany dyrektywy UE w sprawie PNR – standard unijny nie może być niższy niż ten, który przedstawiono w opinii 1/15. Niezależnie od tego, czy mamy do czynienia z wewnętrznym systemem PNR w UE, czy z umowami PNR z państwami trzecimi, szczególnie trudnym wyzwaniem będzie opracowanie systemów, które będą w stanie wprowadzić w życie zaproponowane przez Trybunał rozróżnienia dotyczące zatrzymywania i wykorzystywania danych PNR przed przylotem pasażerów lotniczych, podczas ich pobytu i odlotu oraz po ich odlocie.

Trybunał Sprawiedliwości w swoich orzeczeniach konsekwentnie pokazuje również, że w walce UE z terroryzmem, prywatność i ochrona danych nie zeszły na dalszy plan w stosunku do inicjatyw w zakresie bezpieczeństwa, czego dowodzi nie tylko opinia 1/15, ale także seria orzeczeń w sprawach *Schrems*, w których TS konsekwentnie sprzeciwia się asymetrycznym relacjom między UE a USA, z bardziej dominującą pozycją USA. Jeśli Trybunał dostrzega naruszenia prawa UE, nie ma oporów przed podejmowaniem decyzji, które prowadzą do niezawarcia ważnych umów czy unieważnienia podstaw prawnych współpracy. Trybunał pokazuje przy tym, że interesy bezpieczeństwa i prywatności nie wykluczają się wzajemnie i powinny się przeplatać i uzupełniać.

Literatura

Brkan M., *In Search of the Concept of Essence of EU Fundamental Rights Through the Prism of Data Privacy*, „Maastricht Faculty of Law Working Paper", 2017 nr 1.

Brkan M., *The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning*, „German Law Review German Law Journal" 2019, nr 20

Fantin S., Vogiatzoglou P., Dewitte P., Quezada Tavárez K., *From Theory To Practice: Exercising The Right Of Access Under The Law Enforcement And PNR Directives*, „Journal of Intellectual Property" 2020, nr 11.

Grzelak A., *Główne cele ogólnego rozporządzenia o ochronie danych* [w:] M. Kawecki i T. Osiej, *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, Warszawa 2017.

Grzelak A., *Opinia dotycząca projektu dyrektywy Parlamentu Europejskiego i Rady w sprawie wykorzystania danych dotyczących przelotu pasażera w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich ścigania*, „Zeszyty Prawnicze Biura Analiz Sejmowych" 2011, nr 2

Grzelak A., *Prawo do ochrony danych osobowych a konieczność walki z przestępczością. Uwagi na tle art. 16 traktatu o funkcjonowaniu Unii Europejskiej* [w:] *Prawo Unii Europejskiej a prawo konstytucyjne państw członkowskich*, red. S. Dudzik, N. Półtorak, Warszawa 2013.

Grzelak A., Zielińska K., *Między prawem do prywatności i ochrony danych osobowych a zapewnieniem bezpieczeństwa publicznego i walką z przestępczością. Problemu retencji danych ciąg dalszy - glosa do wyroków Trybunału Sprawiedliwości z 6.10.2020 r.: C-623/17, Privacy International, oraz w sprawach połączonych C-511/18, C-512/18, C-520/18, La Quadrature du Net i in.*, EPS 2021, nr 8.

Guild E., Brouwer E., *The ECJ Decision on the PNR Agreement between the EU and the US*, CEPS Policy Brief, July 2006, nr 109.

Guild E., Mendos Kuşkonmaz E., *EU Exclusive jurisdiction on surveillance related to terrorism and serious transnational crime: case review on Opinion 1/15*, „European Law Review" 2018, vol. 43, nr 4.

Hijmans H., *PNR Agreement EU-Canada Scrutinised: CJEU Gives Very Precise Guidance to Negotiators*, „European Data Protection Law Review" 2017, nr 3.

Hobbing P., *Tracing Terrorists: The EU-Canada Agreement in PNR Matters*, CEPS Special Report, September 2008, revised version 17.11.2008, http://aei.pitt.edu/11745/1/1704.pdf [dostęp: 18.06.2021].

Kuner Ch., *Data Protection, Data Transfers, and International Agreements: the CJEU's Opinion 1/15* [w:] Verfassungsblog, 26 July 2017, verfassungsblog.de [dostęp: 25.11.2021].

Kuner Ch., *Court of Justice International agreements, data protection, and EU fundamental rights on the international stage: Opinion 1/15, EU-Canada PNR*, „Common Market Law Review" 2018, vol. 55, nr 3.

Kusak M., Wiliński P., *Ochrona danych osobowych w ściganiu przestępstw. Standardy krajowe i unijne*, Warszawa 2020.

Lowe D., *The European Union's Passenger Name Record Data Directive 2016/681: Is It Fit for Purpose?*, „International Criminal Law Review" 2016, nr 16.

Maruhashi T., *Japan-EU Passenger Name Record Negotiations and Their Implications* [w:] *Human-Centric Computing in a Data-Driven Society. 14th IFIP TC 9 International Conference on Human Choice and Computers*, red. D. Kreps, T. Komukai, T.V. Gopal, K. Ishii, HCC14 2020, Tokyo, Japan, September 9–11, 2020, Proceedings, Springer 2020.

Mendez M., *Constitutional Review of Treaties: Lessons for Comparative Constitutional Design and Practice*, „International Journal of Constitutional Law" 2017.

Mendez M., *Opinion 1/15: The Court of Justice Meets PNR Data (Again!)*, „European Papers" 2017 vol. 2, nr 3.

Mendez M., *Passenger Name Record Agreement*, „European Constitutional Law Review" 2007, vol. 3, nr 1.

Papakonstantinou V., De Hert P., *Repeating the Mistakes of the Past Will Do Little Good for Air Passengers in the EU: The Comeback of the EU PNR Directive and a Lawyer's Duty to Regulate Profiling*, „New Journal of European Criminal Law" 2015, nr 2.

Papakonstantinou V., De Hert P., *The PNR Agreement and Transatlantic Anti-Terrorism Cooperation: No Firm Human Rights Framework on Either Side of the Atlantic*, „Common Market Law Review" 2009.

Roda S., *Shortcomings of the Passenger Name Record Directive in Light of Opinion 1/15 of the Court of Justice of the European Union*, „European Data Protection Law Review 2020", nr 1

Rojszczak M., *Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*, Warszawa 2019.

Schwartz P.M., *The EU-US Privacy Collission: A Turn to Institutions and Procedures*, „Harvard Law Review" 2013.

Vedaschi A., *The European Court of Justice on the EU-Canada Passenger Name Record Agreement*, „European Constitutional Law Review" 2018, vol. 14, nr 2.

Wiewiórowski W., *Surveillance for public security purposes. Four pillars of acceptable interference with the fundamental right to privacy* [w:] *Data Protection and Privacy under Pressure*, red. G. Vemueulen, E. Lievens, Maklu 2017.

Wojnowska-Radzińska J., *Legitimizing Pre-Emptive Data Surveillance under EU Law – the case of the PNR Directive*, RPEiS 2021, z. 1.
Woods L., *Transferring Personal Data Outside the EU: Clarification from the ECJ?,* EU Law Analysis, 4 August 2017, eulawanalysis.blogspot.co.uk [dostęp: 25.11.2021].

Streszczenie

Agnieszka Grzelak

Przyszłość współpracy UE z państwami trzecimi w sprawie przekazywania danych pasażerów lotniczych. O skutkach opinii Trybunału Sprawiedliwości nr 1/15 dla wymiany danych PNR

System przekazywania danych pasażerów linii lotniczych właściwym organom państwowym do celów związanych z walką z terroryzmem i poważną przestępczością zaczął się w Unii Europejskiej rozwijać, odkąd Stany Zjednoczone zaczęły się domagać takich informacji. W efekcie, Unia Europejska rozpoczęła proces przygotowania umów z państwami trzecimi, które pozwalałyby na przekazywanie takich danych, jak i tworzenia wewnątrzunijnego systemu wymiany danych. W opinii 1/15 dotyczącej umowy z Kanadą, która miała być zawarta przez Unię, Trybunał Sprawiedliwości wyraźnie dopuścił tworzenie systemów wymiany danych PNR, jednakże obwarował to istotnymi ograniczeniami i gwarancjami, które miałyby zapewnić wysoki poziom ochrony prywatności i danych osobowych obywateli UE. W efekcie, do zawarcia umowy z Kanadą nie doszło, negocjacje z innymi państwami zostały wstrzymane. Jednocześnie umowy UE z USA i Australią obowiązują mimo tego, że zawierają sformułowania analogiczne do tych, które uznane zostały przez TSUE za niezgodne z Kartą Praw Podstawowych Unii Europejskiej i Traktatem o funkcjonowaniu Unii Europejskiej. Celem artykułu jest zarówno dokonanie przeglądu tej sytuacji, jak i próba spojrzenia na skutki opinii 1/15 dla systemu wymiany danych PNR w Unii Europejskiej.

Słowa kluczowe: dane PNR; zwalczanie terroryzmu; opinia 1/15; ochrona danych osobowych; RODO.

Summary

Agnieszka Grzelak

The Future of EU Cooperation with Third Countries on the Transfer of Passenger Names Records. On the Effects of the Opinion No. 1/15 of the Court of Justice of the EU on the Exchange of PNR Data

The system for transferring passenger data to the competent state authorities for the purpose of combating terrorism and serious crime began to develop in the European Union after the United States had requested such information from the air carriers. As a result, the European Union started the process of preparing agreements with third countries that would allow the transfer of such data, as well as setting up an intra-EU system for the exchange of data. In the Opinion 1/15 on the agreement with Canada, which was to be concluded by the European

Union, the Court of Justice explicitly allowed for setting up PNR data exchange systems, but subjected this to important limitations and guarantees that would ensure a high level of protection of the privacy and personal data of EU citizens. As a result, the agreement with Canada has not been concluded and negotiations with other countries have been put on hold. At the same time, EU agreements with the US and Australia remain in force, despite the fact that they contain provisions analogous to those found by the CJEU to be incompatible with the Charter of Fundamental Rights of the European Union and the Treaty on the Functioning of the European Union. The aim of this article is to review this situation, but also to analyze the implications of the Opinion 1/15 for the system of PNR data exchange in the European Union.

Keywords: PNR data; combating terrorism; Opinion 1/15; personal data protection; GDPR.